JURNAL DASI ISSN: 1411-3201
Vol. 12 No. 1 MARET 2011

PENERAPAN *NETWORK POLICY* DI INSTANSI PENDIDIKAN UNTUK REMAJA GUNA PENERAPAN INTERNET SEHAT

Sudarmawan, Robert Marco
STMIK AMIKOM Yogyakarta
sudarmawan@amikom.ac.id

ABSTRAKSI

Saat ini banyak sistem jaringan komputer di institusi pendidikan belum optimal karena masalah *network policy* yang belum efektif dan efisien dalam menunjang kinerja suatu organisasi sebagai institusi pendidikan. Menyusun *network policy* di institusi pendidikan bukanlah pekerjaan sederhana, terlebih lagi user yang kompleks menyebabkan proses penyusunan menjadi semakin kompleks. Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Sayang sekali masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting.

Didalam penetapan proxy server yang akan digunakan untuk menfilter/memblokir situs yang akan diakses pada instansi pendidikan. Dimana proxy server adalah sebuah komputer server atau program komputer yang dapat bertindak sebagai komputer lainnya untuk melakukan permintaan terhadap situs/content dari internet. Dalam penelitian ini tujuan dari penggunaan proxy server yaitu untuk menerapkan kebijakan dalam mengakses ke layanan jaringan atau konten dalam melakukan pemblokiran situs-situs yang tidak di izinkan.

Pemakai dapat melakukan pendaftaran untuk mengaktifkan layanan ini. Dalam proses memblokiran ini, banyak jenis pilihan yang dapat ditentukan untuk mendefinisikan situs yang dikategorikan dalam larangan pengaksesan. Dalam melakukan proses pengupdatean jumlah list dengan mencari website yang akan dimasukan dalam whitelist harus dilakukan secara manual, sehingga dalam pengupdate dilakukan secara berkala. Dalam melakukan penambahan tidak harus dilakukan dari admin tetapi dalam dilakukan oleh piahk-pihak lain yang peduli terhadap dukungan penerapan internet sehat.

Kata Kunci : internet sehat, *network policy*

PENDAHULUAN

Teknologi informasi dan telekomunikasi berkembang dengan pesat. Perkembang tersebut telah memberikan banyak dampak dan sumbangsih dalam kehidupan kita. Perkembangan teknologi dan manusia yang menguasainya seolah bermata dua, di satu sisi banyak keuntungan yang dapat didapatkan dari pemanfaatannya, tapi di sisi lain teknologi dapat disalah gunakan baik untuk kepentingan perorangan, kelompok maupun korporasi baik bersifat perdata dan ataupun pidana. Karena jaringan komputer Internet yang sifatnya publik dan global pada dasarnya tidak aman. Pada saat data terkirim dari suatu terminal asal menuju ke terminal tujuan dalam Internet, data itu akan melewati sejumlah terminal yang lain yang berarti akan memberi kesempatan pada user Internet yang lain untuk menyadap atau mengubah data tersebut. Sistem keamanan jaringan komputer yang terhubung ke Internet harus direncanakan dan dipahami dengan baik agar dapat melindungi sumber daya yang berada dalam jaringan tersebut secara efektif. Sistem keamanan jaringan (*network security*) semakin meningkat seiring dengan tingginya kebutuhan untuk itu. Hal ini terjadi akibat meluasnya penggunaan internet dan banyaknya perusahaan yang telah mengimplementasikan teknologi informasi berbasis jaringan pada bisnis mereka.

Internet adalah jaringan publik yang terdiri dari berbagai tipe dan sifat pengguna. Sehingga dibutuhkan suatu cara untuk mengamankan jaringan komputer kita. Salah satu cara yang dapat digunakan untuk mengamankan jaringan adalah dengan memaksimalkan fungsi *firewall* pada komputer kita. *Internet firewall*, dengan segala kelebihan maupun kekurangannya, adalah salah satu mekanisme pengamanan yang paling banyak dipakai saat ini. Internet merupakan media komunikasi yang paling diminati, di Indonesia 64% pengguna internet adalah remaja usia 15-19 tahun. Remaja merupakan usia dimana anak tidak lagi merasa di bawah tingkat orang-orang yang lebih tua melainkan berada dalam tingkatan yang sama. Dalam penelitian ini penulis mengambil subyek remaja, karena menurut data demografi remaja merupakan populasi yang besar dari penduduk dunia. Menurut *World Health Organitation* (WHO) (1995) sekitar seperlima dari penduduk dunia adalah remaja berumur 10-19 tahun. Di Indonesia menurut Biro Pusat Statistik (1999) kelompok umur 10-19 tahun adalah sekitar 22%, yang terdiri dari 50,9% remaja laki-laki dan 49,1% remaja perempuan (Soetjiningsih, 2004). Survei yang dilakukan oleh Yayasan Kita dan

 ISSN: 1411-3201

Buah Hati di Jabodetabek (2005) dengan 1.705 responden remaja memperoleh hasil bahwa lebih dari 80% anak usia 9-12 tahun telah mengakses materi pornografi melalui situs-situs internet.

Saat ini banyak sistem jaringan komputer di institusi pendidikan belum optimal karena masalah *network policy* yang belum efektif dan efisien dalam menunjang kinerja suatu organisasi sebagai institusi pendidikan. Menyusun *network policy* di institusi pendidikan bukanlah pekerjaan sederhana, terlebih lagi user yang kompleks menyebabkan proses penyusunan menjadi semakin kompleks. Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Sayang sekali masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting. Apabila menggangu performansi dari sistem, seringkali keamanan dikurangi atau ditiadakan (Patrick W. Dowd, and John T. McHenry, 1998).

Menurut G. J. Simons (1996), keamanan informasi adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik. Untuk melihat keamanan sistem Internet perlu diketahui cara kerja sistem Internet. Antara lain, yang perlu diperhatikan adalah hubungan antara komputer di Internet, dan protokol yang digunakan. Internet merupakan jalan raya yang dapat digunakan oleh semua orang (*public*). Untuk mencapai server tujuan, paket informasi harus melalui beberapa sistem (*router, gateway, hosts*, atau perangkat-perangkat komunikasi lainnya) yang kemungkinan besar berada di luar kontrol dari kita. Setiap titik yang dilalui memiliki potensi untuk dibobol, disadap, dipalsukan (Budi Rahardjo, 1998). Kelemahan tersebut sistem terletak kepada komponen yang paling lemah.

Penelitian ini akan menganalisa, menjelaskan serta menerapankan suatu Masalah *Network Policy*, Bagaimana Menyusunnya, Mengimplementasi, Serta Mengelolanya Secara Efektif Dan Efisien, guna untuk penerapan penggunaan internet sehat pada instansi pendidikan khususnya pada remaja, serta mengoptimalan Kinerja Dan Keamanan Dapat Tercapai. Dalam penelitian ini akan sedikit banyak mengupas tentang penyalahgunaan teknologi (khususnya jaringan) dan bagaimana cara untuk melakukan penelusuran terhadap penyalahgunaan tersebut.

TINJAUAN PUSTAKA

Penelitian tentang masalah suatu keamanan jaringan komputer di suatu institusi pendidikan yang di titik beratkan pada pengguna (*user*) khusus nya para remaja. Untuk itu diperlukan penerapan *Network Policy* sebagai salah satu tool yang penting dalam sistem layanan jaringan komputer. Pada penenlitian ini akan lebih di fokuskan pada masalah yang akan di hadapi seputar *network policy*.

Network Policy

Tiga Kesalahan Utama Konsep *Network Policy*

1. Tujuan utama *network policy* adalah untuk mengamankan Jaringan Komputer, mengamankan jaringan pada dasarnya bukanlah tujuan utama dari *network policy*, yang menjadi tujuan utama adalah bagaimana mengamankan proses kegiatan yang ada di dalam organisasi tersebut, agar dapat mendukung proses kegiatan menjadi lebih efektif dan efisien dengan menurangi resiko akibat kesalahan user, administrator, serta pihak-pihak yang terkait di dalamnya. *Network policy* menydiakan blueprint tentang apa yang harus diamankan, bagaimana cara mengamankannya untuk mendukung proses kegiatan atau misi yang ada di dalamnya dengan bantuan berbagai teknologi dan konfigurasi seperti Firewalls, intrusion detection sistems (IDS), anti-virus (AV), *backup and restore strategies*, *locked doors*, and sistem administration checklists.
2. *Network policy* harus panjang, lengkap, dan kompleks. Pada kenyataannya, *network policy* yang efektif dan efisienlah yang bertahan lebih baik. *Network policy* yang kompleks biasanya tidak proporsional dan pada umumnya diabaikan. *Network policy* yang baik adalah kumpulan dokumen yang dipisahkan berdasarkan berdasarkan spesifikasi kebutuhan dan pada siapa ditujukan, pengelola, user, atau pihak ketiga. Dengan memisahkan tujuan policy-nya akan lebih mudah diserap oleh audience sesuai dengan tanggung jawabnya masing-masing.
3. *Network policy* harus 100% lengkap dan merupakan pekerjaan sekali jadi. Pada kenyataannya *network policy* adalah proses dan evaluasi berkelanjutan, bahkan dinamika dalam sebuah organisasi ikut menetukan perubahan dalam *network policy*, karena tentunya kebijakan baru akan sejalan dengan

 ISSN: 1411-3201

munculnya kelemahan dan ancaman baru dalan sistem jaringan. Oleh sebab itu *network policy* adalah pekerjaan yang tidak pernah akan berakhir.

Proses Penyusunan *Network Policy*

Tahap pertama dalam penusunan *security policy* adalah pembentukan *team*. Biasanya proses penulisan *network policy* adalah dengan pendekatan top-down process, meskipun ini bukan merupakan syarat mutlak karena pendekatan campuran antara *top-down* dan *bottom-up* memungkinkan untuk diterapkan. Teamwork yang dibentuk sebaiknya terdiri dari para personil yang erat kaitannya dengan aplikasi yang berjalan di atas jaringan tersebut, tidak hanya para personil yang paham akan aplikasi teknologi yang dipakai tetapi juga para personil yang mengerti betul seluk beluk bisnis proses di institusi tersebut, sehingga masing-masing personil memiliki kontribusi yang unik sesuai dengan latar belakang bidang yang dimilikinya untuk menghasilkan network policy yang efektif dan efisien.

Kerangka Network Policy

Pada bagian ini akan dibahas mengenai inti dalam penulisan network policy, setiap institusi tentunya akan menghasilkan policy yang berbeda-beda, namun policy tersebut pada dasarnya akan merujuk pada kerangka tertentu, antara lain sebagai berikut :

1. Seberapa sensitif informasi harus ditangani.
2. Bagaimana maintenance ID, Password, dan seluruh account data penting.
3. Bagaimana merespon potensi security incident dan percobaan gangguan sistem keamanan.
4. Bagaimana menggunakan workstation dan internet dengan cara yang benar.
5. Bagaimana manajemen email sistem.

Adapun bagian-bagian pada network policy berdasarkan kerankanya yang harus diamankan:

1. Komputer Acceptable Use, yakni dokumen yang bersifat umum yang mencakup seluruh penggunaan komputer oleh user, termasuk server dan aplikasi yang berjalan di atas jaringan tersebut.
2. Password, yakni deskripsi tentang persyaratan dalam penggunaan password untuk keamanan komputer dan aplikasinya, bagaimana cara pemilihan password yang tepat, dan bagaimana password policy tersebut di implementasikan.
3. Email, Policy yang mengatur mengenai penggunaan email, mencakup seluruh persyaratan untuk mengoptimalkan email sistem yang ada.
4. Web, yakni policy yang mengatur tentang spesifikasi web browser yang boleh digunakan, bagaimana cara meng implementasikanya, bagaimana konfigurasinya, dan segala policy yang mengatur tentang pembatasan akses pada situs-situs tertentu.
5. Mobile Computing and Portable Storage, yakni deskripsi tentang persyaratan penggunaan mobile computing dan portable storage, bagaimana mensupport device tersebut dan spesifikasi device yang diijinkan untuk digunakan dalam sistem network.
6. Remote access, yakni deskripsi tentang persyaratan penggunaan remote access, siapa saja yang boleh menggunakan, spesifik lokasi, dan segala persyaratan keamanan.
7. Internet, yakni deskripsi tentang konfigurasi gateway, apa saja yang dibolehkan masuk dan keluar gateway, dan mengapa?
8. Wireless, yakni policy yang mengatur megenai wireless sistem, konfigurasi, persyaratan penggunaan, maintenance, pengamanan, dan kondisi penggunaan.
9. Servers, statement dari institusi mengenai standart penggunaan server, tujuan dari spesifik server tertentu, enabled/disabled services.
10. Incident Response Plan, tentunya policy tidak akan pernah lengkap tanpa Incident Response Plan policy, deskripsi tentang apa yang harus dilakukan ketika keamanan jaringan mengalami kegagalan, siapa yang bertanggung jawab, bagaimana penanggulangannya, dan siapa yang memiliki kekuasaan penuh dalam proses ini.

Tujuan *Network Policy*

Untuk lebih mengoptimalkan network policy yang dibuat, maka perlu diketahui apasajakah factor-faktor yang harus dipenuhi, ditujukan pada siapa, dan cakupan wilayah kerjanya.

1. *The institution name*, apakah network policy berlaku untuk seluruh bagian dari institusi, hanya fakultas tertentu saja, jurusan tertentu saja, atau bahkan hanya untuk bagian tertentu dari jurusan tertentu.
2. *The purpose of the policy*, apa tujuan dari network policy, untuk apa? Dan apa yang diharapkan dari dari penyususnan network policy? Missal, untuk tujuan keamanan, atau untuk pengoptimalan kinerja.

 ISSN: 1411-3201

3. *The individuals or organizations responsible for the policy*, siapa yang bertanggung jawab untuk keseluruhan keamanan jaringan, IT Departement atau Sistem Informasi Departement.

Peraturan dalam *Network Policy*

1. *Penalties for breaking policy*, detail tentang hukuman atau sanksi bagi para pelanggar *network policy*, mulai dari peringatan hingga pemecatan.
2. *Who enforces the policy*, seluruh manajemen dan user harus memiliki tanggung jawab yang spesifik pada peraturan yang ada di *network policy*.
3. *How to request policy changes*, detail tentang bagaimana proses perubahan *network policy*, bagaimana cara mengubahnya, siapa yang merevisi, dan parameter apa yang dipakai untuk merevisi *network policy*.
4. *How often your policies must be reviewed*, seberapa sering *network policy* dievaluasi?

Contoh *Network Policy* di Institusi Pendidikan.

The Acceptable use policy

1. Pegawai, dosen, mahasiswa dan pasca sarjana diberi fasilitas email dengan domain masing – masing.
2. Account mahasiswa dan dosen bersifat seterusnya tetapi kapasitasnya dibatasi sesuai dengan kebijakan Jurusan/Fakultas. Untuk account pegawai bersifat sementara selama masih bekerja.
3. Mahasiswa yang melanjutkan studi ke jenjang yang lebih tinggi mendapatkan email baru sesuai dengan jenjang studinya.
4. *Username* email ditentukan sendiri oleh user, sedangkan password diberikan oleh admin. Password tersebut harus segera diganti untuk menghindari penyalahgunaan account email.
5. User yang melaporkan lupa password ke admin wajib mengganti password-nya.
6. *Username* dan password proxy sama dengan username dan password email. Password proxy dapat di ubah, tetapi username tidak bisa diubah – ubah.
7. Semua user yang menggunakan internal workstation wajib men-setting password protected screen saver.
8. Semua user yang akan meninggalkan komputer atau workstation dalam waktu lebih dari 3 menit dan dengan jarak lebih dari pandangan untuk melihat komputernya wajib menjalankan lock screen / logout user.
9. Komputer menggunakan OS linux yang terpusat di server dengan account proxy sebagai autentikasi.
10. Komputer lab tidak diijinkan meng-install software selain yang berkepentingan (asisten dosen lab dan admin)
11. Tidak ada user yang diijinkan untuk meng-copy file sistem operasi (contoh : file SAM, etc/passwd) yang ada di workstation kecuali admin.

Internet Sehat

Internet merupakan suatu jaringan informasi dan komunikasi yang global. Banyak terdapat sejuta manfaat yang akan kita dapatkan hanya dengan bermodal kamauan dan kemampuan dalam menggunkan internet. Misalnya kita dapat berinteraksi dengan berbagai oaring dari seluruh penjuru dunia, serta bias mendapatkan informasi dari berbagai Negara. Kita juga bias mandapatkan data atau informasi baik untuk sekolah/kampus, pekerjaan, mendapatkan informasi atau pun berita baik dalam maupun luar negri, mencari pekerjaan, beasiswa bahkan mengali ilmu tentang agama pun ada, dan masih banyak lagi.

Tentu saja tidak seluruh isi di dalam internet bermanfaat, andai kita dapat memanfaatkannya. Karena sifat internet yang cenderung bebas tanpa di control maupun dikuasai pihak manapun, maka ada saja materi atau informasi yang dapat dikirim maupun di akses melalui internet yang bersifat negative. Misalnya pornografi, perjudian, kekerasan dan rasialisme. Belum lagi dengan adanya program jahat serperti: worm, virus , trojanhourse, dll. Yang dapat mencuri bahkan merusak sistem, baik pelanggaran privasi, penipuan dan pelecehan seksual.

Tetapi dengan adanya pemahaman dan kedewasaan dalam penggunaan internet baik dalam memilah hal yang baik dalam menggunakan internet. Maka kita dapat memaksimalkan dampak positif dengan meminimalakan dampak negative dalam penggunaan internet.

Pasti semua pihak memiliki andil dalam membantu, menyediakan atau menyelengarkan internet yang aman dan nyaman bagi anak-anak dan remaja, seperti:

1. Orang tua harus sering mendampingi anak dalam penggunaan internet di rumah.
2. Guru/ dosen harus senantiasa membimbing siswa/mahasiswa nya dalam penggunaan internet dilingkungan sekolah maupun kampus.

 ISSN: 1411-3201

3. Komunitas, baik pengelolah warnet (warung Internet), lembaga kursus komputer, pelaksana program ektra-kurikuler dan sebagainya, dapat memebantu dalam mendedikasi masyarakat dalam berinternet sehat.
4. Anak-anak, remaja maupun siswa/mahasiswa dapat belajar bertanggung jawab atas prilaku sendiri termasuk ketika menggunakan internet dengan pengawasan orang tua, guru maupun komunitas.

HASIL DAN PEMBAHASAN

Pada saat sebuah instansi pendidikan telah atau akan mengintegrasikan jaringannya secara terpusat untuk keperluan proses pendidikan dengan menggunakan jaringan public (Internet), Maka ada suatu permasalahan lain yang sangat krusial yaitu ”Keamanan atau Security”. Karena tidak ada yang sistem yang aman didunia ini selagi masih dibuat oleh tangan manusia, mengapa karena kita hanya membuat meningkatkan dari yang tidak aman menjadi aman dan biasanya keamanan akan didapat setelah sistem diketahui oleh hacker atau cracker, serta dengan adanya berbagai ancaman banyak sekali seperti Virus, Trojan, Worm, DoS, hacker, cracker, carder, sniffing,defaced, Buffer Overflow, dan sebagainya. Ada banyak teknologi yang menawarkan security jaringan ini. Masing-masing teknologi yang ditawarkan tersebut mempunyai dasar yang sama, yaitu untuk melindungi sistem jaringan dari akses yang tidak berhak dan membatasi suatu layanan yang sesuai dengan policy dari instansi pendidikan.

Selain itu juga dengan penggunaan keaman jaringan yang canggih harus didukung pula dengan prilaku atau sikap para pengguna internet. Pada penelitian ini lebih mengfokuskan pada remaja yang merupakan objek utama, dimana para user remaja terdapat keinginan atau rasa penasaran dengan hal-hal yang baru, untuk itu harus lebih dilakukan pengawasan serta bimbingan tentang penggunaan internet sehat.

Penelitian ini mungkin akan membuka wawasan kita tentang pentingnya ”network policy terhadap keamanan sistem komputer dan untuk Kebijakan Keamanan sistem komputer”. Kesadaran yang penuh dari semua pengguna internet yang merupakan factor utama dalam mengatasi adanya gangguan pada jaringan. Dalam keamanan informasi, ada tiga kategori umum dari kebijakan yaitu:

.

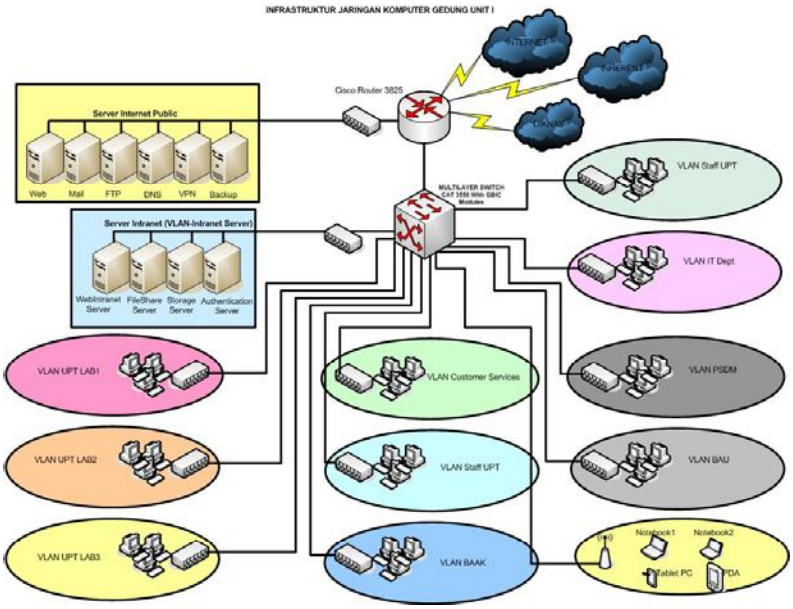
- *Enterprise Information Security Policy (EISP)* menentukan kebijakan departemen keamanan informasi dan menciptakan kondisi keamanan informasi di setiap bagian organisasi.
- *Issue Spesific Security Policy (ISSP)* adalah sebuah peraturan yang menjelaskan perilaku yang dapat diterima dan tidak dapat diterima dari segi keamanan informasi pada setiap teknologi yang digunakan, misalnya e-mail atau penggunaan internet.
- *Sistem Spesific Policy (SSP)* pengendali konfigurasi penggunaan perangkat atau teknologi secara teknis atau manajerial.

Kebijakan keamanan, dimana Semua kejadian pelanggaran keamanan dan setiap kelemahan sistem informasi harus segera dilaporkan dan administrator harus segera mengambil langkah-langkah keamanan yang dianggap perlu. Akses terhadap sumber daya pada jaringan harus dikendalikan secara ketat untuk mencegah akses dari yang tidak berhak. Akses terhadap sistem komputasi dan informasi serta periferalnya harus dibatasi dan koneksi ke jaringan, termasuk logon pengguna, harus dikelola secara benar untuk menjamin bahwa hanya orang/ peralatan yang diotorisasi yang dapat terkoneksi ke jaringan. Semua prosedur serta proses-proses yang terkait pada usaha-usaha pengimplementasian keamanan informasi di perusahaan. Misalnya prosedur permohonan ijin akses aplikasi, prosedur permohonan domain account untuk staf/karyawan baru dan lain sebagainya. Serta harus di dukung dengan tanggung jawab atau responsibility di sini adalah tercerminnya konsep dan aspek-aspek keamanan informasi. Begitu pula dengan adanya program-program pelatihan serta pembinaan tanggung jawab keamaan penggunaan internet di instansi pendidikan untuk staf dan pengguna internet dalam instansi pendidikan.

Topologi Jaringan

Topologi jaringan yang digunakan pada penelitian adalah jenis topologi star yang merupakan jaringan yang sebuah terminal pusat bertindak sebagai pengatur atau pengendali pada semua komunikasi data yang terjadi. Pemilihan topologi berguna untuk merancang bentuk fisik jaringan, menentukan tempat-tempat yang berhubungan dengan jaringan dan menentukan lokasi penempatan komponen jaringan. Terminal pusat akan menyediakan jalur komunikasi khusus untuk dua terminal yang akan berkomunikasi

 ISSN: 1411-3201



Gambar 3.1 Topologi Jaringan

Proxy server

Didalam penetapan proxy server yang akan digunakan untuk menfilter/memblokir situs yang akan diakses pada instansi pendidikan. Dimana proxy server adalah sebuah komputer server atau program komputer yang dapat bertindak sebagai komputer lainnya untuk melakukan permintaan terhadap situs/content dari internet. Dalam penelitian ini tujuan dari penggunaan proxy server yaitu untuk menerapkan kebijakan dalam mengakses ke layanan jaringan atau konten dalam melakukan pemblokiran situs-situs yang tidak di izinkan. Pada sebuah proxy akan focus pada web proxy yang digunakan untuk melayani sebuah web cache. Dalam program proxy menyediakan cara untuk menolak akses ke URL yang akan ditetapkan sebagai data hitam atau black list yang akan tidak di izinkan untuk memasuki situs tersebut, sehingga akan menyaring konten di dalam instansi pendidikan.

Didalam menfilter konten web proxy dengan menyediakan pengatur administrative yang akan di sampaikan melalui proxy, hal ini digunakan untuk memastikan bahwa pengguna internet telah sesuai dengan *acceptable use policy*.

Ada beberapa metode yang akan digunakan untuk memfilter konten yang tidak di izinkan yaitu meliputi: URL atau DNS Black list, URL filter regex, MIME penyaringan, konten filter kata kunci.

Konfigurasi Proxy Server

Dalam membangun sebuah proxy server pada penelitian ini menggunakan sistem operasi OBSD, Program aplikasi Squid, program antarmuka webmin dan di integrasikan dengan menggunakan program nawala.

1. **Program konfigurati Squid proxy**

```
wawan# pw groupadd squid
wawan# pw useradd squid –g squid –d /nonexistent –s /usr/sbin/nologin
wawan# cd /usr/ports/www/squid/
wawan# make config
pilihlah options yang akan disertakan dalam tahap instalasi squid anda,
saya menambahkan options sebagai berikut :
SQUID_DELAY_POOLS # enable delay pools
SQUID_SNMP # enable snmp support
SQUID_HTCP # enable htcp support
SQUID_VIA_DB # enable forward/via database
SQUID_CACHE_DIGEST # enable cache digest
SQUID_UNDERSCORES # allow underscores in hostname
SQUID_USERAGENT_LOG # enable user-agent header logging
SQUID_ARP_ACL # enable acls based on ethernet address
SQUID_PF # enable transparent proxying with PF
SQUID_IPFILTER # enable transp. Proxying with IPFilter
SQUID_LARGEFILE # support log and cache files > 2 GB
```

```
SQUID_RCNG # install an rc.d style startup script
Lalu tekan OK
wawan# make install clean (tunggu sampai proses instalasinya selesai)
wawan# cd /usr/local/etc/squid
sekarang edit file squid.conf
wawan# ee squid.conf
```

untuk lebih enaknya hapus saja semua baris yg ada di file squid.conf, lalu kita coba create sendiri parameter-parameter yang akan kita masukkan di file ini. Berikut isi dari squid.conf saya :

```
http_port 3128
icp_port 3130
htcp_port 4827
icp_query_timeout 2000

maximum_icp_query_timeout 2000
mcast_icp_query_timeout 2000
dead_peer_timeout 30 seconds
hierarchy_stoplist cgi-bin ?
acl QUERY urlpath_regex cgi-bin \?
cache_effective_user squid
cache_effective_group squid

cache_mem 64 MB
cache_swap_low 90
cache_swap_high 95
maximum_object_size 10000 KB
minimum_object_size 0 KB
maximum_object_size_in_memory 32 KB
ipcache_size 2048
ipcache_low 90
ipcache_high 100

fqdncache_size 2048
cache_replacement_policy heap LRU
memory_replacement_policy heap LRU

acl magic_words1 url_regex –i 202.*.*.*/* 192.*.*.*/24
acl magic_words2 url_regex –i ftp .exe .mp3 .vqf .tar.gz .gz .rpm .zip
.rar
.avi .mpeg mpe .mpg .qt .ram .rm .iso.raw .wav

delay_pools 1
delay_class 1 2
delay_parameters 1 -1/-1 -1/-1
delay_access 1 allow magic_words1
delay_class 1 1
delay_parameters 1 1500/4000 1500/4000
delay_access 1 allow magic_words2

cache_dir diskd /cache/ 7000M 24 256 Q1=64 Q2=72
cache_dir diskd /cache2/ 7000M 24 256 Q1=64 Q2=72

cache_access_log /var/log/access.log
cache_log /var/log/cache_log
cache_store_log none
pid_filename /var/run/squid.pid
debug_options ALL,1
log_fqdn off

dns_nameservers 192.*.*.*
query_icmp on
logfile_rotate 10
```

 ISSN: 1411-3201

```
request_header_max_size 100 KB
request_body_max_size 10 MB
refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^http:// 15 20% 43200
refresh_pattern ^ftp://.*/$ 15 20% 10080
refresh_pattern ^ftp:// 15 20% 43200
refresh_pattern . 15 20% 43200

visible_hostname…… (isi kan institusi anda)

acl localip dst 192.168.*.*/255.255.255.0
acl server src 202.138.*.*/255.255.255.240
acl office src 192.168.*.*/255.255.255.0
# acl sesuai dengan ip address user
acl admin src 192.168.*.5
acl wawan src 192.168.*.93
. …... … ……
. …... … ……
# dst. sesuaikan dengan kebutuhan

# acl sesuai dengan departemen yang di inginkan
acl sekretaris url_regex -i “/usr/local/etc/squid/sekre”
acl gudang url_regex -i “/usr/local/etc/squid/gudang”
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl ssl_port port 443 563
acl safe_port port 80 21 443 563 70 1025-65535
acl CONNECT method CONNECT
# allow access
http_access allow wawan
http_access allow admin
http_access allow joni gudang
http_access allow nini sekretaris
http_access deny all

miss_access allow office
miss_access allow server
miss_access allow localhost
miss_access allow manager
miss_access deny all

icp_access allow server
icp_access allow office
icp_access allow localhost
icp_access allow manager
icp_access deny all

maximum_single_addr_tries 5

snmp_port 3401
snmp_access allow server
snmp_access allow office
snmp_access allow localhost
snmp_access allow manager
snmp_access deny all

cache_mgr (isi dengan e mail kita)

memory_pools on
# setting untuk transparent proxy pada squid versi 2.5
httpd_accel_host virtual
httpd_accel_port 80
```

 ISSN: 1411-3201

```
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
# setting transparent proxy pada squid versi 2.6
# ip 192.168.*.* merupakan ip local dari router anda
# http_port 192.168.*.*:3128 transparent
logfile_rotate 10
icp_hit_stale off
ie_refresh off

setelah semuanya terisi dengan benar, lalu save.
wawan# mkdir /cache; mkdir /cache2
wawan# chown squid:squid /cache
wawan# chown squid:squid /cache2
wawan# /usr/local/sbin/squid –k parse
wawan# /usr/local/sbin/squid –z
wawan# ee /etc/rc.conf
tambahkan baris-baris dibawah ini:
ipfilter_enable=”YES”
ipnat_enable=”YES”
ipmon_enable=”YES”
ipfs_enable=”YES”
setelah itu save.
wawan# ee /etc/ipnat.rules
tambahkan baris dibawah ini:
rdr xl1 0/0 port 80 -> 192.168.*.* port 3128 tcp
xl1 => merupakan ethernet local anda
192 => merupakan ip local anda
```

Konfigurasi kernel agar mendukung diskd

Mengenai cara untuk konfigurasi ulang kernel bisa dibaca di http://www.smkn4ptk.net/modul/menginstall%20freebsd.html.

Edit kernel anda, di sini saya menggunakan kernel hasil kompilasi ulang saya sendiri.

```
wawan# cd /usr/src/sys/i386/compile/kernelwawan
wawan# ee GENERIC
tambahkanlah baris-baris dibawah ini:
options SYSVMSG
options MSGMNB=8192
options MSGMNI=40
options MSGSEG=512
options MSGSSZ=64
options MSGTQL=2048
```

Jalankan Squid mu!

```
wawan# /usr/local/sbin/squid –D &
wawan# ee /etc/rc.local
```

tambahkan baris dibawah ini agar squid otomatis jalan ketika pc nyala:

```
/usr/local/sbin/squid –D &
```

Untuk memastikan apakah squid sudah berjalan dengan baik, lakukan pengecekan sebagai berikut:

```
wawan# ps aux|grep squid
root 542 0.0 2.1 4728 2512 ?? Is 2:04PM 0:00.00 /usr/local/sbin/squid -
D
squid 544 0.0 16.3 21700 19928 ?? S 2:04PM 0:49.22 (squid) -D (squid)
squid 550 0.0 0.4 1172 540 ?? Is 2:04PM 0:00.01 (unlinkd) (unlinkd)
squid 551 0.0 0.8 1860 956 ?? Ss 2:04PM 0:01.53 diskd 557056 557057
557058
squid 552 0.0 0.8 1860 936 ?? Ss 2:04PM 0:01.46 diskd 557060 557061
557062
squid 562 0.0 0.9 1520 1060 ?? Ss 2:04PM 0:00.22 (pinger) (pinger)
root 1040 0.0 0.8 1472 976 p0 R+ 4:45PM 0:00.00 grep squid
```

 ISSN: 1411-3201

Setelah itu cobalah gunakan browser anda, dan masukkan URL yang anda kehendaki, apabila terbuka berarti anda sudah berhasil memiliki proxy server di pc anda.

Program aplikasi antarmuka Webmin

Ini adalah script untuk membuat tampilan "informasi anda" seperti yang ada di website ilmuwebsite.com, dalam script ini akan menampilkan :

1. IP
2. Proxy
3. Koneksi

Silahkan memodifikasi script ini

```
<?php
$agent = $_SERVER['HTTP_USER_AGENT'];
$uri = $_SERVER['REQUEST_URI'];
$user = $_SERVER['PHP_AUTH_USER'];
$ip = $_SERVER['REMOTE_ADDR'];
$ref = $_SERVER['HTTP_REFERER'];
$proxy = $_SERVER['HTTP_X_FORWARDED_FOR'];
$via = $_SERVER['HTTP_VIA'];
?>

<table width="140" border="0" style="border-collapse:collapse;">
<tr>
<td background="img/ket_2.jpg">

<img src="img/h_3.jpg" class="menu_kanan"><b>Informasi Anda</b>:
</td>
</tr>
<tr>
<td>
<span><b>IP:</b></span><br> <span style="padding-left:5px;"><?php echo
$ip; ?></span>
</td>
</tr>
<tr>
<td>
<span><b>Proxy:</b></span><br> <span style="padding-left:5px;"><?php
echo $proxy; ?
></span>
</td>
</tr>
<tr>
<td>
<span><b>Koneksi:</b></span><br> <span style="padding-left:5px;"><?php
echo $via; ?
></span>
</td>
</tr>

</tr>
</table>
```

2. **Nawala**

   Gunakanlah alamat DNS berikut ini dan isikanlah alamat IP berikut: 180.131.144.144 pada Preferred DNS server dan 180.131.145.145 pada Alternate DNS server

Proses pemblokiran dapat dilakukan pada proxy. Pemblokiran dengan proxy berlaku untuk semua pengguna yang menggunakan proxy yang telah disetting. Pemblokiran dengan proxy sangat penting terutama untuk komputer yang ada di kantor, sekolah ataupun warung internet. Layanan blokir ini bersifat gratis dan online. Pemakai dapat melakukan pendaftaran

 ISSN: 1411-3201

untuk mengaktifkan layanan ini. Dalam proses memblokiran ini, banyak jenis pilihan yang dapat ditentukan untuk mendefinisikan situs yang dikategorikan dalam larangan pengaksesan. Dalam melakukan proses pengupdatean jumlah list dengan mencari website yang akan dimasukan dalam whitelist harus dilakukan secara manual, sehingga dalam pengupdate dilakukan secara berkala. Dalam melakukan penambahan tidak harus dilakukan dari admin tetapi dalam dilakukan oleh piahk-pihak lain yang peduli terhadap dukungan penerapan internet sehat.

PENUTUP

Network policy tentang penggunaan internet sehat sudah memberikan gambaran lengkap mengenai ketatalaksanaan sistem keamanan pada jaringan internet, tetapi terdapat kesulitan dalam menerapkannya disebabkan kurangnya perhatian banyak orang terhadap pentingnya sistem pengamana jaringan. Kesulitan penerapan ini meliputi pemilihan metode pendekatan untuk risk assessment, melakukan identifikasi resiko, memperkirakan resiko, dan memilih kendali yang tepat untuk diterapkan, serta para pelaku internet (user). Penerapan network policy pada instansi pendidikan tidak selalu komplek dalam pengamanan, dimana harus dilakukan evaluasi atau pemonitoran sistem secara teratur, untuk mencengah terjadinya pelanggaran dalam sistem keamanan.

KESIMPULAN

Berdasarkan dari hasil penelitian dalam penerapan *network policy*, maka diperoleh suatu kesimpulan sebagai berikut:

1. Pembanguan proxy server yang menggunakan fitur pada squid yang digunakan untuk membatasi hak akses para pengguna internet dalam mewujudkan internet sehat dilingkungan pendidikan tidak lepas peran serta dari pengguna itu sendiri dalam mengupdate alamat web secara berkala yang masuk *whitelist* maupun *blacklist.*
2. Dalam pemasukan alamat website yang tidak terdaftar dalam list maka permintaan ke alamat website tersebut akan ditolak.

Saran

Semoga untuk para penelitian kedepan nya agar dapat membuat suatu *network policy* agar dapat melakaukan pembatasan pada penggunaan hak akses pada website secara automatis tanpa dilakukan pemasukan secara manual.

DAFTAR PUSTAKA

Dancho Danchev. Building and Implementing a Successful Information Security Policy.WindowSecurity.Com. 2003.

Frederick M. Avolio and Steve Fallin. Producing Your Network Security Policy. Watchguard.com. July 2007.

Ferdinand Aruan (2003), Tugas Keamanan Jaringan Informasi (Dosen. Dr. Budi Rahardjo) Tinjauan Terhadap ISO 17799 - Program Magister Teknik Elektro Bidang Khusus Teknologi Informasi ITB

Indocommit (23 Desember 2005), Kepatuhan terhadap Sistem Keamanan Informasi http://www.indocommit.com/index.html?menu=29&idnews=506&kid=0&PHPSESSID=ac0fa9bf4b764ea21e26b230102b4ecb,

Jacquelin Bisson, CISSP (Analis Keamanan Informasi, Callio Technologies) & René Saint-Germain (Direktur Utama, Callio Technologies), Mengimplementasi kebijakan keamanan dengan standar BS7799 /ISO17799 untuk pendekatan terhadap informasi keamanan yang lebih baik, White Paper, http://202.57.1.181/~download/linux_opensource/artikel+tutorial/general_tutorials/wp_iso_id.pdf

News Release (April 27, 2006), ISO17799: Standar Sistem Manajemen Keamanan Informasi http://www.nevilleclarke.com/newsReleases/newsController.php?do=toNews&id=45

Puguh Kusdianto (2005), Tugas Akhir EC5010 Keamanan Sistem Informasi, judul Konsep Manajemen Keamanan Informasi ISO-17799 dengan Risk Assessment Menggunakan Metode OCTAVE

Sany Asyari (26 September 2006), Keamanan Jaringan Berdasarkan ISO 17799, *http://sanyasyari.com/2006/09/26/keamanan-jaringan-berdasarkan-iso17799/*

Rahardjo, Budi. "Implikasi Teknologi Informasi dan Internet Terhadapa Pendidikan, Bisnis, dan Pemerintahan: Siapkah Indonesia?", http://budi.insan.co.id/articles/riau-it.doc, 10 September 2006

http://www.sans.org/rr/policy

http://www.secinf.net/policy_and_standards/

http://directory.google.com/Top/Komputers/Security/Policy